JOURNAL OF NUMBER THEORY 3, 247–252 (1971)

On a Problem of Chowla and Shimura

AIMO TIETÄVÄINEN

Department of Mathematics, University of Turku, Turku, Finland

Communicated by S. Chowla

Received March 31, 1970

An answer is given for a problem of Chowla and Shimura concerning congruences of the type

$$a_1x_1^k + \cdots + a_sx_s^k \equiv 0 \pmod{p^h}.$$

1. Let $\Gamma^*(k)$ denote the least integer s with the following property: for each prime power p^h and each sequence of integers $a_1, \ldots, a_s$, the congruence

$$a_1x_1^k + \cdots + a_sx_s^k \equiv 0 \pmod{p^h}$$

has a solution with at least one x_j prime to p. Davenport and Lewis [3] established the result $\Gamma^*(k) \leqslant k^2 + 1$, where there is equality whenever $k + 1$ is a prime (for some further results, see [4]). Chowla [1] was the first to show that $\Gamma^*(k)$ may be much smaller if k is odd. Define

$$\delta = \limsup\{\Gamma^*(k)(k \log k)^{-1}\},$$

where the lim sup is taken over odd k tending to ∞. In [2], Chowla and Shimura proved that

$$1/\log 2 \leqslant \delta \leqslant 2/\log 2$$

and stated that it would be desirable to close the gap between the constants $1/\log 2$ and $2/\log 2$. Norton [5; 6, Section 8] closed this gap halfway, proving the result

$$\delta \leqslant 3/\log 4.$$

It is the purpose of this note to show that

$$\delta = 1/\log 2. \tag{1}$$

In the proof of Lemma 2 we shall use

LEMMA 1. *Let the real numbers* $S(h, j)$, $1 \leqslant h \leqslant q-1$, $1 \leqslant j \leqslant s$, *be such that*

$$S(h, j) \geqslant -u \ (u \geqslant 0),$$

$$\sum_{j=1}^{s} \sum_{h=1}^{q-1} S(h, j) \geqslant 0,$$

and

$$\sum_{j=1}^{s} \sum_{h=1}^{q-1} (S(h, j))^2 = K.$$

Then

$$\sum_{h=1}^{q-1} \prod_{j=1}^{s} (u + S(h, j)) \geqslant (q-1)\, u^s - \tfrac{1}{4} s u^{s-2} K.$$

For a proof of Lemma 1, see [7, p. 4].

3. *Proof of Lemma* 2. Let $G^* = \{\chi_0, \chi_1, \ldots, \chi_{q-1}\}$ be the character group of G (χ_0 is the principal character). Then

$$\sum_{h=0}^{q-1} \chi_h(g) = \begin{cases} q & \text{if } g = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Let A be any one of the sets $G_1, \ldots, G_s$. Denote

$$\chi_h(A) = \sum_{a \in A} \chi_h(a).$$

By assumption (ii), $\chi_h(A)$ is real, and, because $\chi_h(0) = 1$,

$$\chi_h(A) \geqslant -r + 2.$$

Furthermore, by Equation (4) and assumption (i),

$$\sum_{h=0}^{q-1} \chi_h(A) = \sum_{a \in A} \sum_{h=0}^{q-1} \chi_h(a) = q,$$

and hence, by (iii),

$$\sum_{h=1}^{q-1} \chi_h(A) = q - r \geqslant 0.$$

Moreover, it follows from (4), (ii) and (iii) that

$$\sum_{h=0}^{q-1} (\chi_h(A))^2 = \sum_{a \in A} \sum_{b \in A} \sum_{h=0}^{q-1} \chi_h(a + b) = rq.$$

Consequently, by (iii),

$$\sum_{h=1}^{q-1} (\chi_h(A))^2 = r(q - r).$$

Hence we can take in Lemma 1 $S(h, j) = \chi_h(G_j)$, $u = r - 2$ and $K = sr(q - r)$, and we get

$$\sum_{h=1}^{q-1} \prod_{j=1}^{s} (r - 2 + \chi_h(G_j)) \geqslant (q - 1)(r - 2)^s - \tfrac{1}{4}s^2(r - 2)^{s-2} r(q - r). \quad (5)$$

Suppose that, contrary to our assertion, Equation (2) has the trivial solution only. Let $1 \leqslant t \leqslant s$. Let $i_1, \ldots, i_t$ be different elements of the set $\{1, \ldots, s\}$. Because the equation

$$g_{i_1} + \cdots + g_{i_t} = 0, \qquad g_{i_k} \in G_{i_k}$$

has the trivial solution only, we have, by (4),

$$\sum_{g_{i_1} \in G_{i_1}} \cdots \sum_{g_{i_t} \in G_{i_t}} \sum_{h=0}^{q-1} \chi_h \left(\sum_{k=1}^{t} g_{i_k} \right) = q,$$

or

$$\sum_{h=0}^{q-1} \prod_{k=1}^{t} \chi_h(G_{i_k}) = q.$$

Consequently,

$$\sum_{h=0}^{q-1} \prod_{j=1}^{s} (r - 2 + \chi_h(G_j)) = q(r-1)^s. \tag{6}$$

On the other hand, the left side of (6) is, by (5),

$$\geqslant 2^s(r-1)^s + (q-1)(r-2)^s - \tfrac{1}{4}s^2(r-2)^{s-2}\, r(q-r).$$

Combining this with (6), we get

$$q \geqslant 2^s + \left(1 - \frac{1}{r-1}\right)^s \left(q - 1 - \frac{s^2 r(q-r)}{4(r-2)^2}\right). \tag{7}$$

Since $r \geqslant 3$,

$$\frac{r(q-r)}{4(r-2)^2} < \frac{3(q-1)}{2(r-1)}. \tag{8}$$

Furthermore,

$$\left(1 - \frac{1}{r-1}\right)^s \geqslant 1 - \frac{s}{r-1}. \tag{9}$$

In addition, it is rather easy to see, by (6) and (3), that $s < r - 1$. Consequently, by (7), (3), (9), and (8),

$$q > \frac{4s^2(q-1)}{r-1} + q - 1 - \frac{(3s^2 + 2s)(q-1)}{2(r-1)} > q,$$

which is an impossibility. Thus Lemma 2 has been proved.

4. Let $k = k_0 p^f$, where $(k_0, p) = 1$. Define

$$w = \begin{cases} f+2 & \text{if } p = 2, \\ f+1 & \text{otherwise.} \end{cases}$$

Let $s_p(k)$ denote the smallest integer s such that whenever $a_1 \cdots a_s \not\equiv 0 \pmod p$, the congruence

$$a_1 x_1^{\,k} + \cdots + a_s x_s^{\,k} \equiv 0 \pmod{p^w} \tag{10}$$

has a solution with at least one x_j prime to p. Then (see, e.g., [5, p. 100] or [4, p. 183])

$$\Gamma^*(k) \leqslant 1 + k \max\{s_p(k) - 1\},$$

where the maximum is taken over all primes p. Hence for the proof of assertion (1) it suffices to prove the following

LEMMA 3. *For each $\epsilon > 0$, there exists a $k_0(\epsilon)$ such that*

$$s_p(k) < (1 + \epsilon) \log k/\log 2$$

for all odd $k > k_0(\epsilon)$ and for all primes p.

Proof. Consider the congruence (10). Suppose that k is odd and $a_1 \cdots a_s \not\equiv 0 \pmod p$. The proof of case $p = 2$ is trivial (since k is odd, $w = 2$). Hence we may suppose that p is odd. Denote $\delta = (k, \varphi(p^w))$. Let r be the cardinality of the set

$$G_j = \{0\} \cup \{y : 1 \leqslant y < p^w,\ y \equiv a_j x_j^k \pmod{p^w} \text{ for some } x_j \text{ prime to } p\},$$

for some j. Then [5, p. 11]

$$r = 1 + \frac{\varphi(p^w)}{\delta} > 1 + \frac{p^w - 1}{2k}.$$

Because $\varphi(p^w)$ is even, $\varphi(p^w)/\delta \geqslant 2$ and hence $r \geqslant 3$. Thus we may use Lemma 2 with $q = p^w$ and we find that congruence (10) has a solution with at least one x_j prime to p, if

$$2^{s-3} \geqslant s^2 k.$$

This clearly implies Lemma 3.

5. Chowla and Shimura proved in [2] that there is an infinity of odd k such that

$$\Gamma^*(k) \geqslant 1 + k[\log(2k + 1)/\log 2].$$

Norton [5] conjectured that

$$\Gamma^*(k) \leqslant 1 + k[\log(2k + 1)/\log 2]$$

for all odd k. The method used in this paper does not seem to be applicable to a proof of that conjecture.

REFERENCES

1. S. CHOWLA, On a conjecture of Artin I, II, *Norske Vid. Selsk. Forh. (Trondheim)* **36** (1963), 135–141.
2. S. CHOWLA AND G. SHIMURA, On the representation of zero by a linear combination of k-th powers. *Norske Vid. Selsk. Forh. (Trondheim)* **36** (1963), 169–176.

3. H. DAVENPORT AND D. J. LEWIS, Homogeneous additive equations, *Proc. Roy. Soc. Ser. A* **274** (1963), 443–460.
4. M. DODSON, Homogeneous additive congruences, *Philos. Trans. Roy. Soc. London Ser. A* **261** (1967), 163–210.
5. K. K. NORTON, "On homogeneous diagonal congruences of odd degree," Ph.D. thesis, University of Illinois, Urbana, Ill. 1966.
6. K. K. NORTON, Upper bounds for k-th power coset representatives modulo n. *Acta Arith.* **15** (1969), 161–179.
7. A. TIETÄVÄINEN, On a homogeneous congruence of odd degree, *Ann. Univ. Turku. Ser. A. I* **131** (1969), 3–6.

Printed in Belgium